International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 37, No. 4, August, 2020, pp. 671-678
Journal homepage: http://iieta.org/journals/ts

Dynamic Increased Capacity Approach Steganography in Spatial Domain

Aqsa Rashid[1,2], Nadeem Salamat[3*], V.B. Surya Prasath[4]

[1] Department of Information Security, National University of Science and Technology, Islamabad 44000, Pakistan
[2] Department of Computing and Technology, Iqra University, Islamabad 44000, Pakistan
[3] Department of Mathematics, Khwaja Fareed University of Engineering and Information Technology, RahimYar Khan 64200, Pakistan
[4] Department of Electrical Engineering and Computer Science, University of Cincinnati, OH 45221, USA

Corresponding Author Email: nadeem.salamat@kfueit.edu.pk

https://doi.org/10.18280/ts.370417

Received: 25 May 2020
Accepted: 13 August 2020

Keywords:
Gray Level Modification (GLM), information security, Least Significant Bit (LSB), spatial domain, steganography

ABSTRACT

Information security using image steganography is the process of concealing secret information within an image. The conventional methods are static approaches having fixed capacity in term of embedding rate. To solve the problem of static behavior and fixed capacity, we proposed a method that is dynamic approach and increased capacity for embedding rate. Novel algorithm can be used by the data storage industry to design new data storage devices. Other possible applications of this research work will be its usage in other areas such as Watermarking, Document Tracking Tool, Document Authentication Tool, and General Communication etc. Experimental results demonstrate that our proposed steganography algorithm produces the best performance among state-of-the-art algorithms in evaluation of subjective visual assessment as well as objective error metrics.

1. INTRODUCTION

Steganography is paradigm that conceals the secret data into some digital medium in such a way so its existence cannot be noticed by human perception [1-9], see the study [10] for a recent review. With the rapid advancement and use of internet as communication channel, steganography has become an important and valuable tool for secure communication between sender and recipient without the snooping of third person. At the beginning the most known processes of steganography, named as substitution and matching processes, were used for secret communication and many other applications like watermarking, document tracking, document authentication etc. These conventional methods are static approaches having fixed capacity in term of embedding rate. The embedding rate was one bit per pixel for the grayscale images and three bits per pixel for the color images [1-3]. Maheswari and Hemanth [7] utilized Fresnelet transform for frequency domain QR code-based image steganography. Tang et al. [8] proposed a reversible and adaptive image steganographic algorithm based on interpolation. The researches [11-20] present the methods in which least significant bit works and in many methods experiments are performed on different levels of least significant bit position. Luo et al. [21] presents the modified form of LSB substitution by using a secret key. Fridrich [22] and Mielikainen [23] improves the performance of the LSB matching by decreasing the change per pixel. There have been various techniques proposed for steganography. We mention some relevant research techniques here and refer to the study [10] for a comprehensive review of other techniques used in steganography. Subhedar and Mankar [24] utilized wavelet transform and QR factorization from matrix analysis to utilize the redundancy inherent in digital images. Chen et al. [25] utilized principle of the error correction coding channel for devising a data hiding system based on spatial domain least significant bit (LSB) steganography [26], and a capacity analysis model for a MIMO-OFDM coding channel. Yeh et al. [27] considered wavelet bit-plane for steganography for compressed images. Chandramouli and Memon [28] used Shearlet transform and bidiagonal singular value decomposition (SVD) for transparent image watermarking.

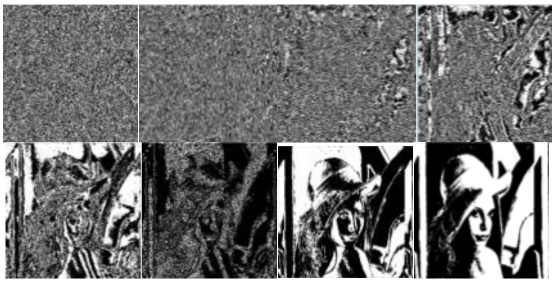


Figure 1. Bit plane view of the gray scale Lena image. As we move from left to right, we move from least to most significant bit plane representation

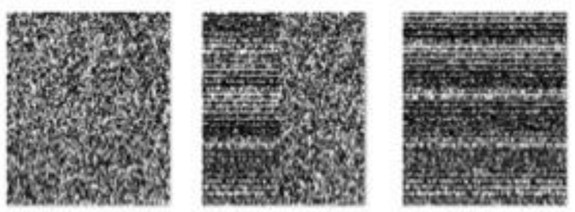


Figure 2. Effect of inconsistency/disturbance in bit plane when static steganography is applied. From left to right: Clear least bit image, and after 50% and 100% static embedding

There are certain problems with the static steganographic approaches. Static Approaches typically create specific patterns in statistical features of the images that makes the syego-system easily breakable. Static methodologies create disturbance in the correlation of the bit planes of the images, creates static pattern in the histogram of the image e.g. pair of values (POV) [29-31] in case of image substitution steganography. Figure 1 shows the bit plane view of the gray scale Lena image. All these bit planes have correlation with each other. As we move from left to right, we are actually moving from least to most significant bit plane. Although any change in least bit planes does not affect the overall visual appearance of the image, but bit plane slice view will clearly show the effect of disturbance in the corresponding bit plane. Figure 2 shows the effect of disturbance/inconsistency in the correlation of the image bit plane when we apply static steganography methods. Left image shows the clear least bit plane of the image. Central image shows the effect of static embedding methodology after 50% embedding rate and right image shows after 100% embedding rate. Static approaches have fixed capacity in terms of embedding rate. This is a problem because embedding capacity for static methodology depends on the size of the image.

For a strong and unbreakable steganography systems, the methodology of the embedding phase should be design in such a way so that the statistical features of the image should not create repeated patterns. In this paper, a new dynamic approach for the grayscale and color images has been presented. The novel method has increased the embedding rate up to 4 bits per pixel for the grayscale images and up to 12 bits per pixel for the color images. The major challenges to design a new approach includes,

- dynamic embedding methodology,
- increased embedding rate,
- and achieve above said challenges with least changes in image quality and security analysis measures.

The testing criteria or tools used for the evaluation of the new proposed approach will be based on Image Quality Measures, Security Analysis, Histogram Analysis and Bit Plane Analysis [32-40].

Rest of the paper is arranged as follows. Section 2 presents the proposed dynamic increase capacity-based method. Section 3 provides detailed experimental results and discussion. In Section 4 we conclude the paper.

2. PROPOSED DYNAMIC INCREASED CAPACITY METHOD FOR STEGANOGRAPHY

Our dynamic increased capacity-based methodology is divided into four phases to achieve the said challenges. Figure 3 shows the phases in sequential order. All the 256 gray levels are analyzed and classified into four categories. Analysis and classification are based on the color depth and maximum payload for that color that will create least statistical changes so that the change remains imperceptible in both objective evaluation and subjective visual assessment.

For each classified group, we use the Mod Function that have dynamic mod factor depending on the number of bits to be embedded in the pixel. Table 1 shows the range of grey levels for all the four categories, their embedding rate, Mod-Function and Mod-Factor.

Formal processing steps for embedding phase include the following sequence:

a) Take the pixel and check its category from Table 1. If it is from Cat. 1 then go to step (b), if it is from Cat.2 then go to step (c), if it is from Cat. 3 then go to step (d) and if it is from Cat.2 then go to step (c).

b) Take the pixel decimal and compute the mod value by using 2 as mod factor. It the binary of mod value and message bit is same then no change required. Otherwise adjust the pixel value in such a way so that the binary of mod value becomes the message bit.

c) Take the pixel decimal and compute the mod value by using 4 as mod factor. It the binary of mod value and message bit is same then no change required. Otherwise adjust the pixel value in such a way so that the binary of mod value becomes the message bit.

d) Take the pixel decimal and compute the mod value by using 8 as mod factor. If the binary of mod value and message bit is same, then no change required. Otherwise adjust the pixel value in such a way so that the binary of mod value becomes the message bit.

e) Take the pixel decimal and compute the mod value by using 16 as mod factor. It the binary of mod value and message bit is same then no change required. Otherwise adjust the pixel value in such a way so that the binary of mod value becomes the message bit.

f) If all the bits are embedded i.e., bit stream is empty now then go to step (g) else go to (a).

g) End

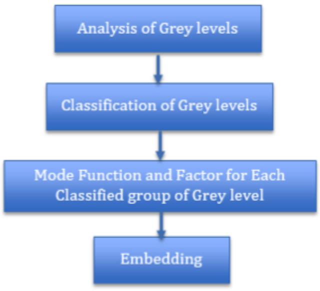

Analysis of Grey levels
Classification of Grey levels
Mode Function and Factor for Each Classified group of Grey level
Embedding

Figure 3. Processing phases of our proposed dynamic increased capacity method

Table 1. Range of gray values

Category	Range	Capacity	Mod-Function	Mod-Factor
Cat.1	0-191	1 Bit	2n where n=1	2
Cat.2	192-223	2 Bits	2n where n=2	4
Cat.3	224-239	3 Bits	2n where n=3	8
Cat.4	240-255	4 Bits	2n where n=4	16

It is important to mention that for all the steps that require adjustment, the adjustment process should not change the category of the grey level after applying adjustment process for embedding. Grey level of the pixel should remain in the same category before and after the adjustment process. Adjustment process is just an increment or decrement in the pixel value so that the message bit and pixel's bit become the equivalent.

Extraction of the message includes the following steps.
Input: Stego image, length of Bit Stream
Output: Bit Stream

a) Take the pixel and check its category from Table 1. If it is from Cat. 1 then go to step (b), if it is from Cat.2 then go to step (c), if it is from Cat. 3 then go to step (d) and if it is from Cat.2 then go to step (c).

b) Compute the mod value of pixel decimal by 2 as mod factor and put the binary of mod value in the bit stream.
c) Compute the mod value of pixel decimal by 4 as mod factor and put the binary of mod value in the bit stream.
d) Compute the mod value of pixel decimal by 8 as mod factor and put the binary of mod value in the bit stream.
e) Compute the mod value of pixel decimal by 16 as mod factor and put the binary of mod value in the bit stream.
f) If the total number of bits in the Bit Stream have been completed, then goes to step (g) else go to (a).
g) End

3. EXPERIMENTAL RESULTS

In this section, we investigate the performance of the proposed algorithm by analyzing some benchmark images. These benchmark images include five grayscale and five color images. We analyze all experiments that are carried out on a database of ten images with the size of 512 x 512. As shown in Figure 4, we number these images from one to ten (according to the order from the left-to-right and top-to-bottom).

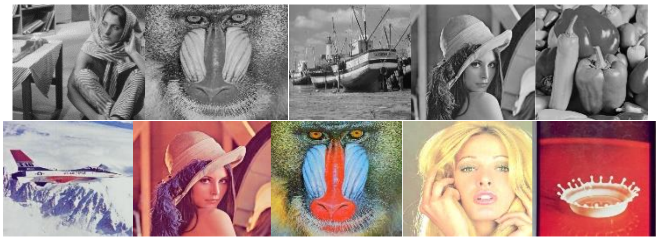


Figure 4. Set of test images – we refer to image 1 to image 10, from left-to-right and top-to-bottom. Note that we chose 5 gray scale and 5 color images representing various image contents, flat regions, texture, and strong edges

Table 2. MSE values of the ten test steganography images after different embedding rates

Image	MSE after 33472 Bits	MSE after 66832 Bits	MSE after 100296 Bits	MSE after 133712 Bits
1	0.0235	0.0454	0.0700	0.0945
2	0.0304	0.0590	0.0838	0.1067
3	0.0304	0.0457	0.0733	0.0959
4	0.0304	0.0413	0.0628	0.0806
5	0.0304	0.0591	0.0841	0.1090
6	0.0253	0.0506	0.0751	0.0984
7	0.0250	0.0943	0.0513	0.1227
8	0.0252	0.0507	0.0746	0.0969
9	0.0482	0.0877	0.1297	0.1883
10	0.0208	0.0423	0.0685	0.0963

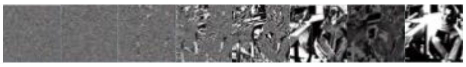
We obtain the steganography images by embedding different embedding rate with the proposed approach. The quality of steganography images is evaluated by using frequently used full-reference image quality assessment methods, such as mean square error (MSE) [6] value and peak signal-to-noise ratio (PSNR) value [6]. Objective performances for ten - five grayscale and five color (RGB - red, green, blue - channels), images are given in Table 2 and Table 3. Less MSE and higher PSNR (dB) values are indicative of better performance. We chose these ten test images that contain various objects and texture characteristics to show the advantages of the proposed dynamic increased capacity approach. We obtained similar results on other standard test images from the image processing literature. Obtained values in Table 2 and Table 3 show that the proposed technique produces very good performance for both the grayscale and color images. The statistical changes are least so that the differences between the original cover and steganography images are undetectable. This assertion is supported by lower MSE values and higher PSNR (dB) values for various test images. We also note that even in the high content texture images such as the Baboon (images 2, 8) we obtained lower MSE values – 0.1067, 0.0969 respectively for gray and color images – at the higher embedding 133712 bits.

Table 3. PSNR (dB) values of the ten test steganography images after different embedding rates

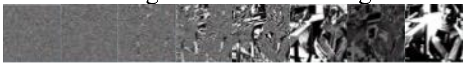
Image	PSNR after 33472 Bits	PSNR after 66832 Bits	PSNR after 100296 Bits	PSNR after 133712 Bits
1	64.4857	61.5679	59.6946	58.3777
2	63.2622	60.3848	58.8769	57.8231
3	64.7686	61.5143	59.4485	58.2932
4	63.7686	61.9906	60.1545	59.0682
5	63.9270	60.3808	58.8533	57.7431
6	63.4078	61.0506	59.3828	58.2013
7	64.0271	57.4773	60.2518	56.3447
8	63.4652	61.4639	59.6563	58.4522
9	60.3815	58.0201	56.5200	55.1808
10	64.9384	61.7694	59.3944	57.7516

3.1 Bit plane analysis

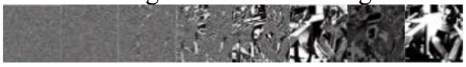
Bit plane analysis checks the visual inconsistency due to any change in the image pixel value. For the most popular methods including LSB substitution [1], LSB matching [2, 3], GLM method [5] etc. the visual inconsistency is clearly visible in least bit planes and for the robust increased capacity image steganography scheme, least two-bit planes show clear change. The projected scheme of steganography has the advantage over these methods that the bit planes does not show the visual inconsistency in the bit planes.



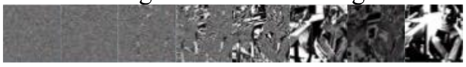
Bit Plane of image 1 after embedding 33472 Bits



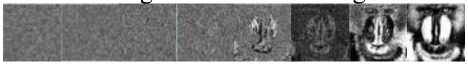
Bit Plane of image 1 after embedding 66832 Bits



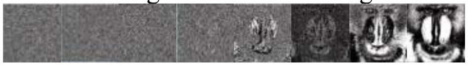
Bit Plane of image 1 after embedding 100296 Bits



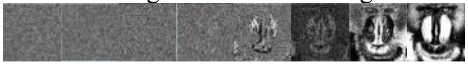
Bit Plane of image 1 after embedding 133712 Bits



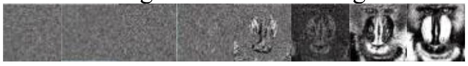
Bit Plane of image 2 after embedding 33472 Bits



Bit Plane of image 2 after embedding 66832 Bits



Bit Plane of image 2 after embedding 100296 Bits



Bit Plane of image 2 after embedding 133712 Bits

Bit Plane of image 3 after embedding 33472 Bits

Bit Plane of image 3 after embedding 66832 Bits

Bit Plane of image 3 after embedding 100296 Bits

Bit Plane of image 3 after embedding 133712 Bits

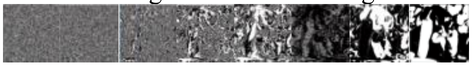
Bit Plane of image 4 after embedding 33472 Bits

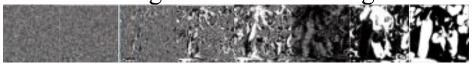
Bit Plane of image 4 after embedding 66832 Bits

Bit Plane of image 4 after embedding 100296 Bits

Bit Plane of image 4 after embedding 133712 Bits

Bit Plane of image 5 after embedding 33472 Bits


Bit Plane of image 5 after embedding 66832 Bits


Bit Plane of image 5 after embedding 100296 Bits

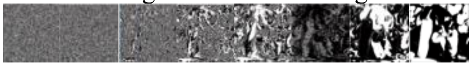
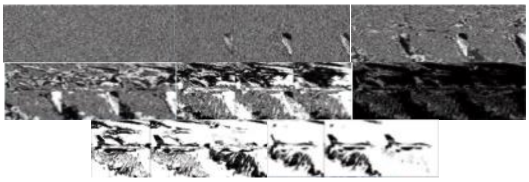
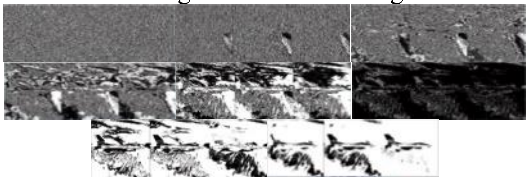
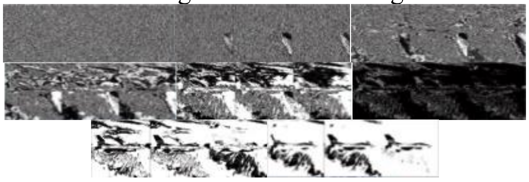
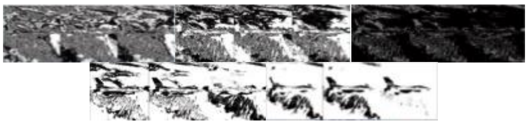

Bit Plane of image 5 after embedding 133712 Bits

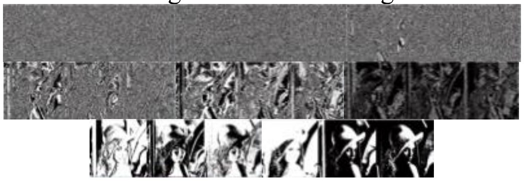
Figure 5. Bit plane analysis for the 5 gray scale test images with various embedding bits – 33472, 66832, 100296, 133712 with our dynamic capacity approach steganography. We show for each test image, bit plane images after these four embedding bits. We see that the final bit plane image does not show any visual inconsistencies

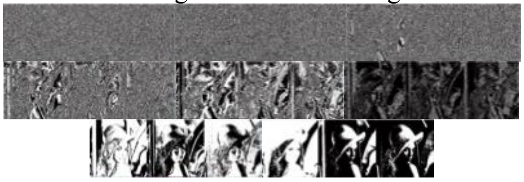

Bit Plane of image 6 after embedding 33472 Bits

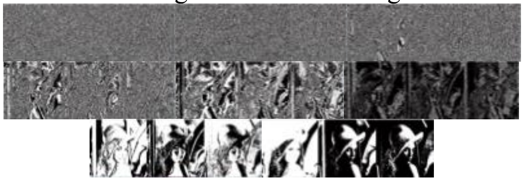

Bit Plane of image 6 after embedding 66832 Bits

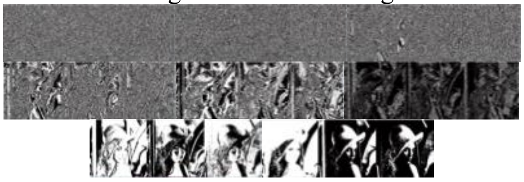

Bit Plane of image 6 after embedding 100296 Bits

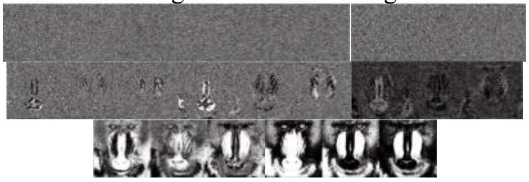

Bit Plane of image 6 after embedding 133712 Bits

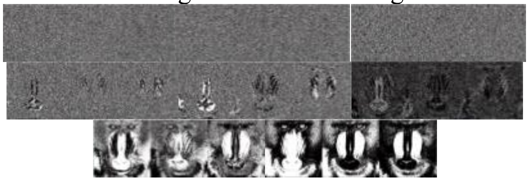

Bit Plane of image 7 after embedding 33472 Bits

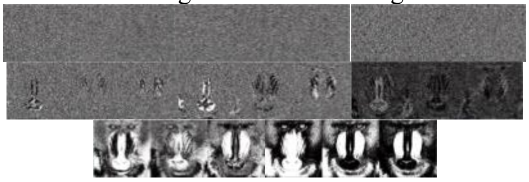

Bit Plane of image 7 after embedding 66832 Bits

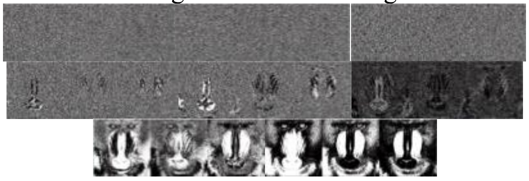

Bit Plane of image 7 after embedding 100296 Bits

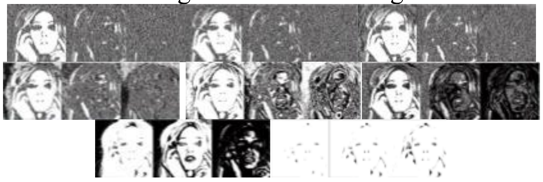

Bit Plane of image 7 after embedding 133712 Bits

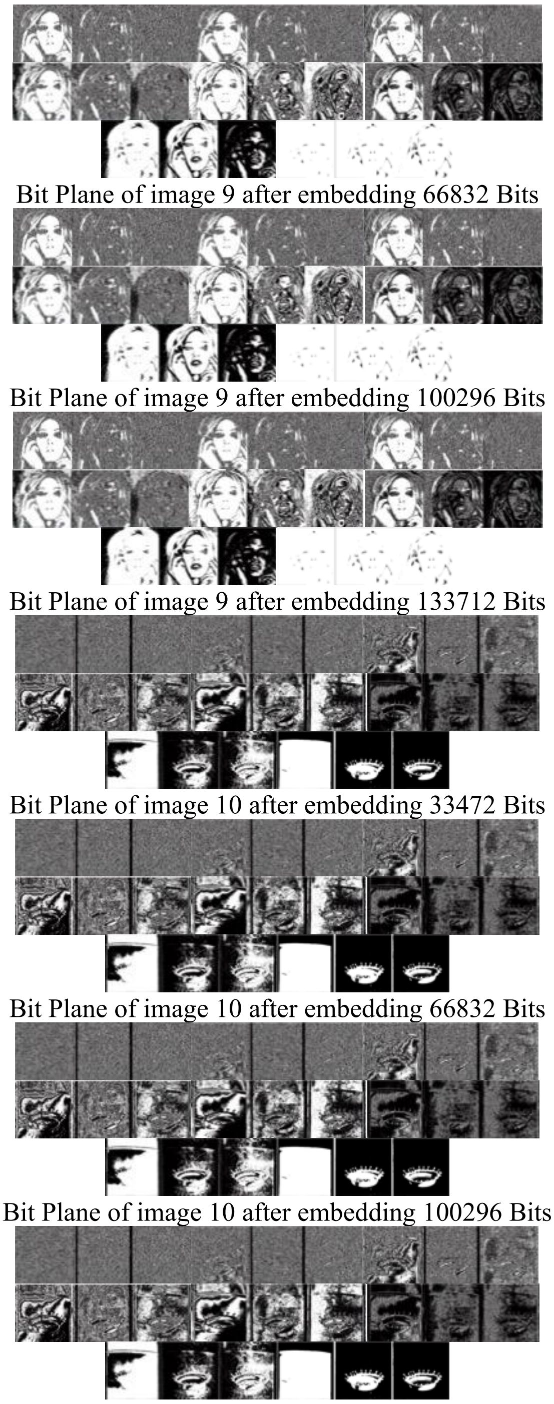

Bit Plane of image 8 after embedding 33472 Bits


Bit Plane of image 8 after embedding 66832 Bits


Bit Plane of image 8 after embedding 100296 Bits


Bit Plane of image 8 after embedding 133712 Bits


Bit Plane of image 9 after embedding 33472 Bits



Bit Plane of image 9 after embedding 66832 Bits

Bit Plane of image 9 after embedding 100296 Bits

Bit Plane of image 9 after embedding 133712 Bits

Bit Plane of image 10 after embedding 33472 Bits

Bit Plane of image 10 after embedding 66832 Bits

Bit Plane of image 10 after embedding 100296 Bits

Bit Plane of image 10 after embedding 133712 Bits

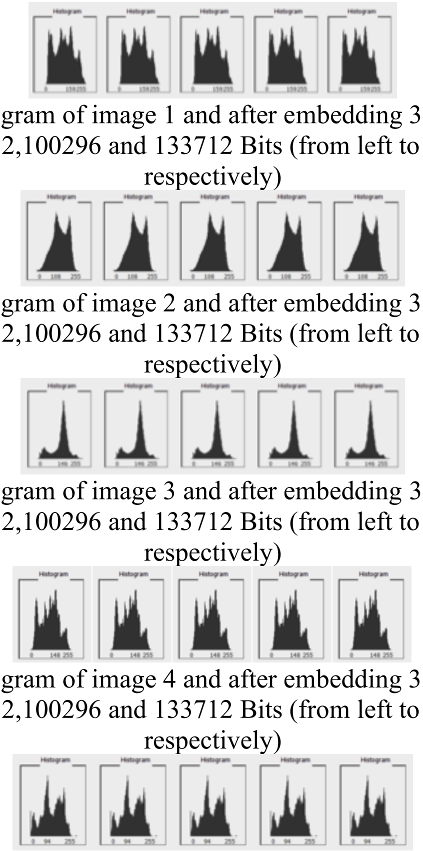
Figure 6. Bit plane analysis for the 5 color test images with various embedding bits – 33472, 66832, 100296, 133712 with our dynamic capacity approach steganography. We show for each test image, bit plane images after these four embedding bits in each color channels

This is since, in the proposed increased capacity approach, the message bits are embedded dynamically. Figure 5 shows the bit planes of images after embedding different bits in the test images from Figure 4. For color images three-bit planes, for red channel, blue channel and green channels, are shown in Figure 6. As can be seen, the proposed approach obtains no visual inconsistencies indicated other models (compare Figure 2) that are manifestation of static steganography methods.

Also, the final bit plane image in both gray scale and color images show that the image features are kept intact, and no artifacts are observed in the resultant images.

3.2 Histogram analysis

Histogram of an image shows the graphical distribution of the picture element value. In image steganography, histogram analysis is used as a steganography analysis tool for various steganography schemes. For LSB substitution [1], LSB matching [2, 3], GLM method [5] etc., histogram creates the specific pattern. For the projected scheme, as the embedding is in dynamic style, so histogram cannot be used as the steganography analysis tool. Histograms of the images after embedding different bits using test images of Figure 1 are shown in Figure 7. For the color images, three channels-based histograms are shown separately in Figure 8. We notice that the histograms do not show any sequenced peaks or discernible patterns that are associated with other related models.



Histogram of image 1 and after embedding 33472, 66832,100296 and 133712 Bits (from left to right respectively)

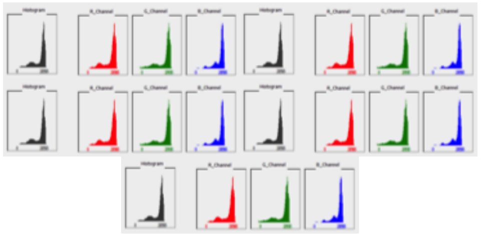
Histogram of image 2 and after embedding 33472, 66832,100296 and 133712 Bits (from left to right respectively)

Histogram of image 3 and after embedding 33472, 66832,100296 and 133712 Bits (from left to right respectively)

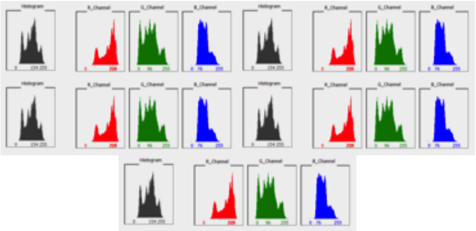
Histogram of image 4 and after embedding 33472, 66832,100296 and 133712 Bits (from left to right respectively)

Histogram of image 5 and after embedding 33472, 66832,100296 and 133712 Bits (from left to right respectively)

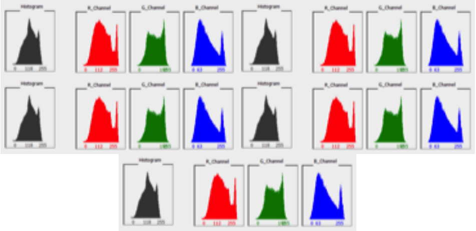
Figure 7. Histogram analysis for the 5 gray scale test images with various embedding bits – 33472, 66832, 100296, 133712 with our dynamic capacity approach steganography. We show for each test image, bit plane images after these four embedding bits



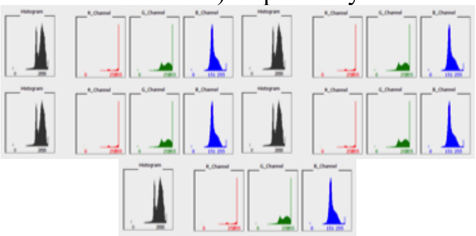
Histogram of image 6 and after embedding 33472, 66832,100296 and 133712 Bits (from left to right and top to bottom) respectively



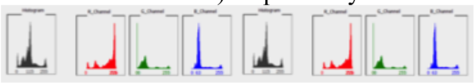
Histogram of image 7 and after embedding 33472, 66832,100296 and 133712 Bits (from left to right and top to bottom) respectively

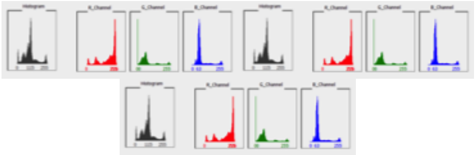


Histogram of image 8 and after embedding 33472, 66832,100296 and 133712 Bits (from left to right and top to bottom) respectively



Histogram of image 9 and after embedding 33472, 66832,100296 and 133712 Bits (from left to right and top to bottom) respectively





Histogram of image 10 and after embedding 33472, 66832,100296 and 133712 Bits (from left to right and top to bottom) respectively

Figure 8. Histogram analysis for the 5 gray scale test images with various embedding bits – 33472, 66832, 100296, 133712 with our dynamic capacity approach steganography. We show for each test image, bit plane images after these four embedding bits

3.3 Comparative analysis

Comparative analysis of the projected method with the LSB substitution [1], LSB matching [2, 3], increased capacity in spatial domain [4] and GLM [5] methods is summarized in terms of bit plane and histogram analysis as well as static versus dynamic, bits per pixel in Table 4. It is clear from the Table 4 that new proposed dynamic increased capacity approach is best in terms of embedding rate, visual analysis and histogram analysis.

From experimental results it can be seen that the proposed dynamic approach obtained better results in terms of lower MSE and higher PSNR (dB) indicating the resultant images are indistinguishable from original images. Compared to other methods, our proposed approach also utilized 4 bits per pixel, whereas the previous models at the top use 3 in the case of color images. In terms of histogram analysis, we see that our proposed method is devoid of artificial structures and the corresponding histograms show no discernible patterns whereas the previous models can create either sequenced peaks or maxima/minima changes.

Table 4. Comparative analysis of the projected method

Stego-System	LSB Substitution [1]	LSB Matching [2, 3]	Increased Capacity in Spatial Domain [4]	GLM Method [5]	Our Proposed Method
Bits Per Pixel	1 for grayscale images, 3 for color images	1 for grayscale images, 3 for color images	2	1 for grayscale images, 3 for color images	Up to 4
Static/ Dynamic	Static	Static	Static	Static	Dynamic
Visual Analysis (Bit Plane Analysis)	Least bit plane has clear Change	Least bit plane has clear Change	Least two-bit planes have clear change	Least bit plane has clear change	Change in bit planes remain invisible
Histogram Analysis	Creates pair of values (POV)	Local maxima of the histogram of image will decrease and the local minima will increase	Histogram does not create specific pattern	Histogram show sequenced peaks which show the presence of information	Undetectable, as histogram does not create any specific pattern

Further, the proposed approach is dynamic in contrast to other static methods for steganography. The least bit planes do not show visible changes, and this is advantageous in for example in medical images category wherein drastic pixel changes are undesirable [37]. Finally, the proposed approach is shown to work on color images that are extensions of gray scale models with increased capacity in the spatial domain. Extending this approach to handle multichannel and multimodal imagery data is an interesting framework that requires further consideration.

4. CONCLUSIONS AND FUTURE WORK

This paper proposes dynamic increased capacity steganography algorithm in spatial domain. We adopt more precise and sophisticated data estimation strategy to evaluate the performance of the projected algorithm. This novel strategy is conducive to data storage industry to design innovative data storage devices. The proposed algorithm has been tested on benchmark images and the experimental results demonstrate that the new algorithm performs best in mean squared error (MSE) value, peak signal to noise ratio (PSNR) measure, measured in decibels (dB), bit plane analysis, histogram analysis, and embedding rate. We believe the proposed algorithm will be of interest on the data storage side, which can also be adopted to develop data storage devices offering more cost and size efficiency with better security. In future, attempt will be made to modify the methodology with some other mathematical models to increase the capacity and at the same time reduce the processing time. Implementation and experimentation of the proposed method for the video files will also be the part of future contribution.

ACKNOWLEDGMENT

We sincerely thank the reviewers for their comments that helped us improve the quality and content.

REFERENCES

[1] Rashid, A., Missen, M.M.S., Salamat, N. (2016). Analysis of steganography techniques using least significant bit in grayscale images and its extension to colour images. Journal of Scientific Research and Reports, 9(3): 1-14. https://doi.org/10.9734/JSRR/2016/19518

[2] Rashid, K.R., Rashid, A., Salamat, N., Missen, M.M.S. (2014). Experimental analysis of matching technique of steganography for grayscale and color images. International Journal of Computer Science & Information Technology, 6(6): 157-166. https://doi.org/10.5121/ijcsit.2014.6613

[3] Rashid, A. (2015). Experimental analysis and comparison of LSB substitution and LSB matching method of information security. International Journal of Computer Science Issues, 12(1): 91-100.

[4] Rahim, M.K., Salamat, N., Missen, S., Rashid, A. (2014). Robust increased capacity image steganography scheme. International Journal of Advanced Computer Science and Applications, 5(11): 125-131. https://doi.org/10.14569/IJACSA.2014.051122

[5] Rashid, A., Rahim, M.K. (2015) Experimental review of "Gray Level Modification". International Journal of Signal Processing, Image Processing and Pattern Recognition, 8(11): 265-272. https://doi.org/10.14257/ijsip.2015.8.11.24

[6] Rashid, A., Rahim, M.K. (2016). Classification, analysis and comparison of non-blind image quality measures. International Journal of Signal Processing, Image Processing and Pattern Recognition, 9(4): 347-360. https://doi.org/10.14257/ijsip.2016.9.4.31

[7] Maheswari, S.U., Hemanth, D.J. (2015). Frequency domain QR code based image steganography using Fresnelet transform. AEU - International Journal of Electronics and Communications, 69(2): 539-544. https://doi.org/10.1016/j.aeue.2014.11.004

[8] Tang, M., Hu, J., Song, W., Zeng, S. (2015). Reversible and adaptive image steganographic method. AEU - International Journal of Electronics and Communications, 69: 1745-1754. https://doi.org/10.1016/j.aeue.2015.08.011

[9] Ramalingam, M., Isa, N.A.M. (2016). A data-hiding technique using scene-change detection for video steganography. Computers & Electrical Engineering, 54: 423-434. https://doi.org/10.1016/j.compeleceng.2015.10.005

[10] Subhedar, M.S., Mankar, V.H. (2014). Current status and key issues in image steganography: A survey. Computer Science Review, 13: 95-113. https://doi.org/10.1016/j.cosrev.2014.09.001

[11] Chan, C.K., Cheng, L.M. (2001). Improved hiding data in images by optimal moderately-significant-bit replacement. IEE Electronics Letters, 37(16): 1017-1018. https://doi.org/10.1049/el:20010714

[12] Chang, C.C., Tseng, H.W. (2004). A steganographic method for digital images using side match. Pattern Recognition Letters, 25(12): 1431-1437. https://doi.org/10.1016/j.patrec.2004.05.006

[13] Chan, C.K., Cheng, L.M. (2004). Hiding data in images by simple LSB substitution. Pattern Recognition, 37(3): 469-474. https://doi.org/10.1016/j.patcog.2003.08.007

[14] Song, X.R., Gao, S., Chen, C.B., Wang, S.L. (2020). A novel face recognition algorithm for imbalanced small samples. Traitement du Signal, 37(3) 425-432. https://doi.org/10.18280/ts.370309

[15] Wang, R.Z., Lin, C.F., Lin, J.C. (2001). Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recognition, 34(3): 671-683. https://doi.org/10.1016/S0031-3203(00)00015-7

[16] Chang, C.C., Hsiao, J.Y., Chan, C.S. (2003). Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. Pattern Recognition, 36(7): 1538-1595. https://doi.org/10.1016/S0031-3203(02)00289-3

[17] Chang, C.C., Chan, C.S., Fan, Y.H. (2006). Image hiding scheme with modulus function and dynamic programming strategy on partitioned pixels. Pattern Recognition, 39(6): 1155-1167. https://doi.org/10.1016/j.patcog.2005.12.011

[18] Chang, C.C., Lin, M.H., Hu, Y.C. (2002). A fast and secure image hiding scheme based on LSB substitution. International Journal of Pattern Recognition and Artificial Intelligence, 16(4): 399-416. https://doi.org/10.1142/S0218001402001770

[19] Thien, C.C., Lin, J.C. (2003). A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. Pattern Recognition, 36(12): 2875-2881. https://doi.org/10.1016/S0031-3203(03)00221-8

[20] Ker, A. (2005). Steganalysis of LSB matching in gray scale images. IEEE Signal Processing Letter, 12(6): 441-444. https://doi.org/10.1109/LSP.2005.847889

[21] Luo, W., Huang, F., Huang, J. (2010). Edge adaptive image steganography based on LSB matching revisited. IEEE Transactions on Information Forensics Security, 5(2): 201-214. https://doi.org/10.1109/TIFS.2010.2041812

[22] Fridrich, J. (2009). Steganography in Digital Media: Principles, Algorithms, and Applications, Cambridge University Press, UK.

[23] Mielikainen, J. (2006). LSB matching revisited. IEEE Signal Processing Letters, 13(5): 285-287. https://doi.org/10.1109/LSP.2006.870357

[24] Subhedar, M.S., Mankar, V.H. (2016). Image steganography using redundant discrete wavelet transform and QR factorization. Computers & Electrical Engineering, 54: 406-422. https://doi.org/10.1016/j.compeleceng.2016.04.017

[25] Chen, L., Fan, Z., Huang, J. (2016). Data hiding capacity

of spatial domain bit replacement steganography in a MIMO-OFDM coding channel. AEU - International Journal of Electronics and Communications, 70(9): 1295-1303. https://doi.org/10.1016/j.aeue.2016.07.004

[26] Beşdok, E. (2005). Hiding information in multispectral spatial images. AEU - International Journal of Electronics and Communications, 59: 15-24. https://doi.org/10.1016/j.aeue.2004.11.040

[27] Yeh, H.L., Gue, S.T., Tsai, P., Shih, W.K. (2016). Wavelet bit-plane based data hiding for compressed images. AEU - International Journal of Electronics and Communications, 67: 808-815. https://doi.org/10.1016/j.aeue.2013.04.003

[28] Chandramouli, R., Memon, N. (2001). Analysis of LSB based image steganography techniques. In IEEE International Conference on Image Processing (ICIP), pp. 1019-1022. https://doi.org/10.1109/ICIP.2001.958299

[29] Wu, D.C., Tsai, W.H. (2003). A steganographic method for images by pixel-value differencing. Pattern Recognition Letter, 24(9-10): 1613-1626. https://doi.org/10.1016/S0167-8655(02)00402-6

[30] Westfeld, A., Potzmann, A. (1999). Attacks on steganographic systems - Breaking the steganographic utilities Ezstego, Jsteg, Steganos, and S-tools-and some lessons learned. In Proceedings of the 3rd Information Hiding Workshop, volume 1768 of LNCS, pp. 61-76.

[31] Provos, N., Honeyman, P. (2002). Detecting steganographic content on the internet. In Proceedings of Network and Distributed System Security Symposium, pp. 1-13. http://hdl.handle.net/2027.42/107898

[32] Avcibas, I., Memon, N., Sankur, B. (2003). Steganalysis using image quality metrics. IEEE Transactions on Image Processing, 12(2): 221-229. https://doi.org/10.1109/TIP.2002.807363

[33] Mardanpour, M., Chahooki, M.A.Z. (2016). Robust transparent image watermarking with Shearlet transform and bidiagonal singular value decomposition. AEU - International Journal of Electronics and Communications, 70: 790-798. https://doi.org/10.1016/j.aeue.2016.03.004

[34] Faragallah. O.S. (2013). Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain. AEU - International Journal of Electronics and Communications, 67: 189-196. https://doi.org/10.1016/j.aeue.2012.07.010

[35] Subhedar, M.S., Mankar, V.H. (2016). Image steganography using redundant discrete wavelet transform and QR factorization. Computers & Electrical Engineering. https://doi.org/10.1016/j.compeleceng.2016.04.017

[36] Rashid, A., Salamat, N., Prasath, V.S. (2019). On a secure steganography approach with increased capacity and security. International Journal of Computer Vision and Signal Processing, 1(1): 1-9.

[37] Rashid, A., Salamat, N., Prasath, V.B.S. (2018). An algorithm for data hiding in radiographic images and ePHI/R application. Technologies, 6(1): 7. https://doi.org/10.3390/technologies6010007

[38] Kumar, S.K., Reddy, P.D.K., Ramesh, G., Maddumala, V.R. (2019). Image transformation technique using steganography methods using LWT technique. Traitement du Signal, 36(3): 233-237. https://doi.org/10.18280/ts.360305

[39] Bikku, T., Paturi, R. (2019). Frequency domain steganography with reversible texture combination. Traitement du Signal, 36(1): 109-117. https://doi.org/10.18280/ts.360114

[40] Gopil, A.P., Narayana, V.L. (2017). Protected strength approach for image steganography. Traitement du Signal, 34(3-4): 175-181. https://doi.org/10.3166/TS.35.175-181